TYPE S1/FULL/2,3,5,6,9,10,12

1/9/2 (Item 1 from file: 15)

02148570 71041550

E-signed, sealed, and delivered

Piazza, Peter

Security Management v45n4 PP: 72-77 Apr 2001 CODEN: SECME6 ISSN: 0145-9406 JRNL CODE: SEM
DOC TYPE: Periodical; Feature LANGUAGE: English RECORD TYPE: Fulltext
LENGTH: 5 Pages
SPECIAL FEATURE: Illustration Photograph
WORD COUNT: 3457

ABSTRACT: Two experiences with public key infrastructure (PKI) offer valuable lessons to businesses looking for ways to secure online transactions. The registration system at MIT was tedious and exasperating for everyone involved. Administrators decided to set up a Web-based system to allow students to preregister for classes by computer. The question was how to make it secure. The answer was PKI, because it offered two critical capabilities: privacy and authentication. Fannie Mae assembled a team that included members of the operations, legal, human resources, network engineering, and e-business departments. This group examined the company's needs and requirements, present and future, to determine exactly what should be protected by the authentication and encryption capabilities that PKI would provide. The team also decided to use PKI to streamline transactions.

TEXT: COMPUTER SECURITY

Two very different institutions roll out public key infrastructures to authenticate users and protect confidential information.

PUBLIC KEY INFRASTRUCTURE (PKI). The mere name of this authentication and encryption system can make the average business person's eyes glaze over. Even among the techno-literate, PKI has an enduring reputation as hard to understand and even harder to implement. But Chrisan Herrod of Fannie Mae is a PKI fan. "It's something that can help you if you let it help you, and you can change your business processes using it," says Herrod, director of information security at Fannie Mae. She should know. She oversaw the rollout of a PKI system at her company, the largest provider of home mortgages funds in the United States. The Massachusetts Institute of Technology (MIT) went through a similar rollout of its own PKI system. The two experiences offer valuable lessons to businesses looking for ways to secure online transactions.

MIT's School Project

TO REGISTER FOR CLASSES, STUDENTS AT MIT, LIKE students everywhere, have in the past had to fill out forms on paper, then stand in long lines in the gym to submit their forms to the registrar. When a class they wanted was fully subscribed, they had to go back to the end of the line, frantically thumbing through paper catalogs to find replacement courses as they made their way again to the front of the line. Meanwhile, the registrar's staff working the lines had to manually enter the information for lo,ooo students into the university's computer database. It was tedious and exasperating for everyone involved.

Assessing needs. Administrators knew that there must be a more efficient

way to get students registered. They decided to set up a Webbased system to allow students to preregister for classes by computer. The question was how to make it secure. The answer was PKI, because it offered two critical capabilities: privacy and authentication.

Blessed with state-of-the-art technology and no shortage of scientific minds, the university created a system from scratch, rather than outsourcing the project, as most businesses would. However, MITs experience in assessing how PKI could benefit them and rolling out the system to thousands of users can be a lesson for any business.
The school's needs were fairly simple, according to Jeffrey Schiller, network manager and security architect for MIT. Students needed a way to prove their identity to register for classes and access the university Web sites, and the university needed a way to ensure that private data on the site, such as financial aid or grades, would be secure.

PKI startup. It took Schiller about a week to write code for the PKI system, which is based on the idea of digital certificates, issued as a form of electronic ID, and public/private key pairs, issued for encryption and decryption. In a PKI system, there must be a trusted relationship with a third party, so that individuals or systems have a basis for trusting each other's messages over a network. Thus, there are three pieces to the PKI puzzle when it comes to the issuance of certificates: the root certificate authority (RCA), the certificate authority (CA), and the end user, which gets issued the certificate and public/private digital key pair. In MIT's case, the university is the CA.

While MIT issues certificates to students, the university itself has been issued a certificate by an RCA, which also happens to have its server on MIT's property. That RCA is called CREN (the Corporation for Research and Educational Networking, a consortium of universities that provides institutional certificate services). CREN certificates are issued when a school registers to be a CA.

The authority to be a CA and issue digital certificates must be carefully controlled if digital certificates are to be trusted forms of identification in the electronic universe. Thus, the server that issues the CREN root certificates is secured inside a hardware box in a locked, alarmed room on MIT's campus. Schiller explains that the CREN server requires an extremely high level of security because if an unauthorized person obtained access, that person could become a CA with the ability to issue digital certificates to anyone-essentially manufacturing fake electronic IDs.

To ensure against the possibility of an unauthorized CA root certificate being issued, the CREN server cannot sign a certificate unless two people insert plastic "crypto-ignition" keys (similar to those used for firing missiles from submarines) at the same time. Schiller has one, kept under two levels of lock and key; the other is similarly secured by the director of academic computing at MIT.

Another part of the picture is an institutional digital key, used by MIT to issue certificates to students. -The tricky part," Schiller says, "is that the server that issues certificates to people is an online service." This unavoidably creates a level of insecurity. This key is encrypted, and though Schiller has made it difficult to steal, he acknowledges that "somebody sufficiently skilled in the arts" could do it. He adds that MIT runs its own network-level intrusion detection system so that the university would be immediately aware of and able to respond to any unauthorized access to the server.

Pilot program. The university tested its electronic ID system in 1996 with a short pilot program involving about ioo students. The pilot went smoothly, and MIT rolled out the system to another 8,ooo students that summer.

All of the participating students received a paper coupon when they arrived on campus, with their name, identification number, and a unique six-word passcode. They used this passcode to access a special MIT Web site residing on the server that was the nerve system of the CA function; once they entered the passcode, which proved their identity, they chose a new user name and password. An automated program (called a wizard) then led the students through a simple process to receive two packets of data that would be used by computers on either side of future transactions to verify the student and the site.
These packets are called digital certificates. Both reside in the browser of the student's computer. The first is an MIT site certificate, which certifies the identities of MIT sites on the Internet. The second packet is a personal certificate, which contains the student's name, the student's user name, the beginning and expiration dates of the certificate, and a certificate serial number. The certificate-holder also gets a public/private key pair. A digital signature, encrypted with the private key, becomes an electronic ID because it can only be decrypted by the corresponding public key.

The student's private key resides on his or her computer, and the student has a password to retrieve it. If anyone obtains the password and gains access to the private key, he or she can impersonate the student.

"That's the weakest link," Schiller says. "However, the tradeoff is that it only affects one person." MIT tells students not to share that information with anybody and that violators of the policy will be held responsible for any negative results.

How it works. If student John Smith wants to check his grades, he'll point his browser to the designated MIT Web site. When he reaches the page, the Web site will challenge his browser to provide John's certificate. If he hasn't used the certificate before in this session, he'll be prompted to enter the password that protects the certificate. This extra safeguard helps to ensure that someone else could not sit at John's computer and impersonate him electronically.

Meanwhile, John's browser will check the MIT site certificate to verify the identity of the site. Through this digital "handshake," both John and the Web site provide authentication of their identities.

Next, the Web server takes John's user name from the certificate and matches it (through an internal database) to his student identification number. Based on that identification, the computer presents him with his records. During this process, John never sees the certificates being used; the process is automatic.

The certificates enable students to use their computers to enter class and housing lotteries, gain access to online libraries and journals, and purchase items at a discount from certain online vendors. The certificates are accepted by third-party vendors, so employees can also use them to purchase office supplies and computer products.

Rollout problems. Unlike many other enterprise PKI projects, MIT moved from pilot to full implementation quickly-in the course of one semester-and with

great success. "We've had maybe loo problems, but we've issued 200,000 certificates, Schiller says, "and that's not a bad ratio." Most of the problems were not serious and involved error messages or crashes caused by improperly configured browsers. A help desk Web site allows users to solve those problems easily.

Key compromise. So far, Schiller says, no student has ever reported the compromise of a private key, but he suspects that may be because students do not understand the need to have the certificate revoked if, for example, a laptop is stolen.

He suspects some laptops have been stolen, "so some have had their keys compromised," he says. "End users don't understand that they have to take an action" by immediately reporting it to the systems administrator so the certificate can be revoked and reissued. The university is trying to address the issue through education.

Key management Key management is a major issue in the administration of a PKI program. Making students aware of the need to report stolen or compromised keys is only one part of the key management challenge. If a student quits the university, MIT will revoke the corresponding certificate. However, that student still has the certificate on his or her computer. It could not be used to log into the registrar's office or access any sensitive sites within MIT. But an outside vendor that had been approached online would have to check a certificate revocation list to know that it should deny the transaction. This is more of a problem with employees whose certificates have been revoked. "If a staff member leaves, we want to make sure they can't go and buy a computer" using their MIT certificate, Schiller says.

Schiller anticipates that some difficulties might also arise when certificates are used among institutions. He explains how different authentication policies can lead to mistrust. "For example, we give [students] a coupon when they arrive that allows them to get a certificate. Another university might decide that a student has to appear before a university official with two forms of picture ID and a notarized statement. The problem is, would that university accept a credential issued by MIT?"

Schiller is not sure how such conflicts will be resolved. He notes that for now the university simply indicates on the certificate how the student's identity was authenticated so that others can make an informed decision about its validity.
Results. Mary Callahan, the registrar of MIT, says that the university has found the effort worthwhile. -Students get a lot more good information online, right in front of them. We can update [the site] if a subject changed its time or got cancelled, so a student gets the most current information, rather than a time-dated paper bulletin."

The new system has also saved her staff from hours of tedious data entry. "Now we do a lot more problem solving," she says. "I feel that we offer a lot better level of service, but it takes a different skill set now to be working in the registrar's office."

MIT moved from pilot program to full implementation of its Pla program in one semester. The program allows students to register for classes online, making the process easier for staff and students.

Targeted PKI

THE FIRST QUESTION THAT FACED FANNIE Mae when it began to consider the use

of an electronic ID system was how extensively to implement PKI. "You don't have to PKI your whole company," Director of Information Security Herrod says. "A lot of people go overboard."
To handle the project, the company assembled a team that included members of the operations, legal, human resources, network engineering, and ebusiness departments. The group examined the company's needs and requirements, present and future, to determine exactly what should be protected by the authentication and encryption capabilities that PKI would provide.

The project team came to several conclusions. First, the company wanted secure e-mail and intranet applications for internal use. Second, it needed to protect sensitive employee data and confidential information about customers. General e-mails about policies or nonsensitive data would not need to be encrypted or digitally signed.

The team also decided to use PKI to streamline transactions. "PKI not only provides encryption but [also] provides the ability to 'sign on the digital line,' so we can sign timecards online," Herrod says. "In the future we can sign purchase orders online, too. We can reduce the workflow tremendously and hence reduce costs and increase efficiencies as well."

The next step was to select a PKI partner. The team created a list of essentials. First, the secure e-mail and any Web-based applications would have to work with Netscape and Microsoft Outlook, which was already standardized in the company. Looking into the future, they wanted to be able to implement a secure remote access method called virtual private network, or VPN, using smart cards or tokens, as well as desktop encryption. They needed a simple rollout that was easy for users and administrators. Finally, they wanted their PKI system to be up and running quickly. The team sent its needs to several PKI vendors. These suppliers then gave presentations. Eventually, the company chose to outsource the project to Entrust.

Starting small. Fannie Mae decided that the best course of action would be to set up an internal PKI system first, and once the infrastructure was working smoothly, to push that out to private lenders, real estate agents, and others who work with the company. By focusing on an internal PKI system first, Herrod and her team could be sure that they completely understood the technology and that they could work through any glitches before getting into client considerations.

Even within the company, Herrod found, the process should be gradual. "Experiment with your rollout procedures before you actually give it to important users in your company," she says. "I would never start with the CEO; always start out with your own team first."
Because it needed an easy-to-use system that was up and running quickly, Fannie Mae decided that Entrust would take care of all the backend infrastructure; it hosted the certificates and set up the policy configuration according to Fannie Mae's needs. Fannie Mae's users and administrators would securely access the certificates through the Web.

Certificate policy. The Fannie Mae team established a certificate policy (CP) and a set of rules addressing concerns such as the CA's key length and how long the certificates would be valid. This CP, says Leah MacMillan, director of product management and marketing for Entrust, made the implementation much easier. "We could look at the CP and make sure that we conformed to everything that they needed to do. Then we could explain how we were going to set up their PKI according to their security policies and desired configuration settings."

Entrust brought a small group of Fannie Mae users to its lab, where a sample system based on the CP was set up. The users checked out all the settings to make sure they were in accordance with what was expected, learned the administrative functions, and saw what kinds of problems arose before the system went live.

The PKI system is integrated with the Netscape browser and Microsoft Outlook e-mail application on each desktop. At first, there were some computer crashes, but these were not completely unexpected, Herrod says. "If you don't have the browser properly configured, you'll have a problem, and it happens quite a bit, no matter what vendor you're using," she says.

Herrod's team realized they needed to change certain Netscape browser security configurations on every desktop to prevent the crashes. They developed an automated script and distributed it via e-mail to users, who only had to double-click on the message to launch a silent install, which would change the browser settings.

Entrust support staff spent about a week in the company, training the system administrators on how to use the system. Two Fannie Mae staff members were given additional duties as registration authorities (RAs), administrators who add and delete users from the system. The RAs completed a short training course in how to load and delete information. Once the RAs received their digital IDs, they could begin to add new users; they could also assign and create additional local RAs to distribute the administrative work as the system expanded.

Two other staff members were designated as revocation authorities. If someone loses a laptop or leaves the company, they revoke the certificate instantly.

Testing. Fannie Mae's RAs selected 500 users to register for digital certificates as a part of a test. Users were selected from departments, such as HR and legal, whose staff handled the type of transactions that would merit PKI security. The RAs sent an e-mail to these users welcoming them and informing them that they would be prompted for a password to get the certificate. (The e-mail explained that the password would be a piece of identifying information that the employee and the registrar would both know but that would not be common knowledge. For example, they might be asked for their mother's maiden name.)

The e-mail then directed each user to click on the Web site address in the message. This launched the browser, and the Web page that opened asked the pilot users to enter their password to begin the creation of their digital ID. The site securely accesses Entrust, which issues and stores their certificates, and the Entrust software in the browser generates public and private keys, which give users the ability to encrypt and sign online. The private key is password protected in the user's browser.

Training. Next, Fannie Mae instituted a training class for its pilot group of 500 users. Trainers explained to the employees who would be issued the certificates exactly why the PKI system was implemented and how it would work. For example, they were told that once they received their certificates, they would simply click on an icon to activate the encryption routine or to digitally sign a document. If an encrypted e-mail arrived, users would simply double-click on it, and the process would occur.

In addition to the training class instituted, Fannie Mae has put information on its Web site that walks users through its policy on when to

useand when not to use-encryption. For example, human resources personnel are told to encrypt messages containing salary data, legal information, and medical data. Users are taught to apply PKI based on commonsense rules and practices, Herrod explains. They are told: "If you think this is too sensitive to send via e-mail, then encrypt it," she says.

Rollout. One of Fannie Mae's longterm goals is to encrypt sensitive records and restrict user access to that data, using the same PKI system. "Privacy is a huge issue, and we want to make sure that we're protecting private information," says Herrod. "We have tremendous databases where we store information about homebuyers, and that's something we're obligated under the law to protect."

To give staff a chance to try out their certificates, Fannie Mae posted its code of conduct on a Web site, and each user digitally signed it. As the company rolls out the program to the rest of the staff, it has set up lunchtime learning sessions by department to walk users through the encryption feature. The training and the rollout are continuing incrementally, and by the end of 2002, every full-time Fannie Mae employee-about 4,000 peoplewill have a certificate. In the future, the company intends to use smart cards or tokens rather than passwords to enhance the security of the user's private key.

Future impact. Fannie Mae is working with the Mortgage Bankers Association of America and the American Bankers Association to create the Real Estate Finance (REF) Trust Network, a community-of-interest certificate authority on behalf of the real estate finance industry. Through the REF Trust Network, certificates can be issued to accredited institutions that can then do e-business together.

PKI makes business more efficient, Herrod says. That, she notes, will eventually benefit homebuyers as well by creating a paperless mortgage application process.

As these case studies illustrate, setting up electronic ID and encryption systems can be a challenge. But the rewards of automating such routine tasks as student registration and loan applications can pay great dividends down the digital road.

Peter Piazza is assistant editor of Security Management

Apr 2001
COMPANY NAMES:
Fannie Mae (DUNS:04-951-5430 TICKER:FNM NAICS:522294)
Massachusetts Institute of Technology (DUNS:00-142-5594 NAICS:611310)
GEOGRAPHIC NAMES: United States; US

DESCRIPTORS: Computer security; Public Key Infrastructure; Case studies; Colleges & universities; Mortgage companies
CLASSIFICATION CODES: 5140 (CN=Security); 9190 (CN=United States); 9110 (CN=Company specific); 8306 (CN=Schools & educational services); 8120 (CN=Retail banking)
PRINT MEDIA ID: 19213

1/9/3 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

08408769 Supplier Number: 71554994 (THIS IS THE FULLTEXT)

Cylink, Securant to Offer Integrated PKI-based Solution To Bolster Web Security.

Business Wire, p2132
March 12, 2001
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 795

TEXT:

Business Editors/High-Tech Writers

SANTA CLARA, Calif.--(BUSINESS WIRE)--March 12, 2001

Cylink's NetAuthority PKI and Securant's ClearTrust SecureControl to Provide Central, Tailored Access of Web-based Applications

Cylink Corporation (Nasdaq:CYLK), a leading provider of e-business security solutions, has partnered with Securant Technologies to offer an integrated public key infrastructure-based solution that allows enterprises, government agencies and application service providers to centrally control and tailor access to Internet-based applications, content and transactions.

Under the agreement, Cylink will ensure that its NetAuthority public key infrastructure (PKI) solution is compatible with Securant's ClearTrust SecureControl access management system. The integrated solution will provide enterprises with a single auditable point of control for managing access to PKI-secured Internet and extranet applications for employees, customers and partners.

Using easy-to-follow on-screen instructions, users of the integrated solution will authenticate to ClearTrust SecureControl via industry-standard X.509 certificates issued by NetAuthority. ClearTrust SecureControl's security policy management infrastructure (PMI) streamlines authorization by enabling users to sign on once for access to any number of Web applications instead of having to rely on separate usernames and passwords for each, regardless of operating platform. In addition to bolstering security, the PMI, which can be configured to limit access to pre-determined applications, reduces the costs associated with replacing forgotten or otherwise obsolete usernames and passwords. NetAuthority provides the trusted environment for user authentication to PMI and a number of other Internet-based applications.

"The Cylink-Securant solution will combine two compelling sets of features to provide the security needed for highly trusted web-based communications," said William P. Crowell, President and CEO of Cylink. "The strong user authentication of Cylink's NetAuthority PKI and the central access control of Securant's security policy management infrastructure will provide an easy-to-use platform for tailoring access to Internet applications."

"As enterprises move high-value transactions and business-critical applications onto the Internet, PKI provides the level of trust and security required to protect these sensitive resources from misuse and fraud," said Eric Olden, Securant's Chief Technology Officer. "The integration of Cylink's NetAuthority solution with our ClearTrust SecureControl access management system will maximize the authentication capabilities of PKI and give enterprises the confidence to provide single sign-on Web access to precious applications and resources."

NetAuthority is a highly scalable, standards-based infrastructure incorporating public-key cryptography, certificates, digital signatures and encryption to enable a wide variety of applications including secure email and web browsing and virtual private networking. Designed to support intranet, extranet and Internet applications, NetAuthority consists of a certificate authority, registration server, registration authority client and a toolkit that can make any device and application PKI-compatible.

ClearTrust SecureControl enables enterprises to centrally manage

PKI-based authentication to protect both Web-based and Web-presented applications. In addition, ClearTrust SecureControl can manage and deliver multiple security services that integrate with PKI. To provide real-time security enforcement and prevent unauthorized access, the PMI solution supports Certificate Revocation List (CRL) checks to deny access to users with revoked or suspended certificates.

About Securant

Securant Technologies, the access management company that secures e-business, is a leading provider of Internet security software for managing user access to Web-based resources including applications, content and transactions. Securant customers include Merrill Lynch, Baker Street, Chase Hambrecht & Quist, Lehman Brothers, Experian, MarketFusion, Scientific Atlanta and Thomson Financial. To contact Securant, call 415/315-1500, visit www.securant.com, or write to info@securant.com.

About Cylink Corporation

Cylink Corporation develops, markets and supports a comprehensive family of e-business security solutions. Founded in 1983, the company was the first to market security solutions that protect communications with public key cryptography. Cylink and its wholly owned subsidiaries serve Fortune 500 companies, multinational financial institutions, and government agencies worldwide. To contact Cylink, call 408/855-6000 or visit www.cylink.com.

Some of the statements in this announcement involve risks and uncertainties, and actual results could be materially different. The statements concerning the parties' future product offerings and their capabilities are forward looking statements. Among the factors that could cause actual results or developments to differ are unexpected delays in product developments, failure of the market to accept new products or technologies, difficulty in hiring and retaining qualified personnel, and other risk factors listed from time to time in the company's SEC reports, including but not limited to the report on Form 10-K, Forms 10-Q, and the Annual Report to shareholders.

Note to Editors: Cylink is a registered trademark of Cylink Corp.

PUBLISHER NAME: Business Wire
COMPANY NAMES: *Cylink Corp.
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *3662000 (Communications Equipment ex Telephone)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
SIC CODES: 3660 (Communications Equipment)
NAICS CODES: 3342 (Communications Equipment Manufacturing)
TICKER SYMBOLS: CYLK
SPECIAL FEATURES: LOB; COMPANY

1/9/5 (Item 2 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

15565841 (THIS IS THE FULLTEXT)
Cylink, Securant to Offer Integrated PKI-based Solution To Bolster Web Security
BUSINESS WIRE
March 12, 2001
JOURNAL CODE: WBWE LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 738

SANTA CLARA, Calif.--(BUSINESS WIRE)--March 12, 2001--
Cylink's NetAuthority PKI and Securant's ClearTrust SecureControl

to Provide Central, Tailored Access of Web-based Applications

Cylink Corporation (Nasdaq:CYLK), a leading provider of e-business security solutions, has partnered with Securant Technologies to offer an integrated public key infrastructure-based solution that allows enterprises, government agencies and application service providers to centrally control and tailor access to Internet-based applications, content and transactions.

Under the agreement, Cylink will ensure that its NetAuthority public key infrastructure (PKI) solution is compatible with Securant's ClearTrust SecureControl access management system. The integrated solution will provide enterprises with a single auditable point of control for managing access to PKI-secured Internet and extranet applications for employees, customers and partners.

Using easy-to-follow on-screen instructions, users of the integrated solution will authenticate to ClearTrust SecureControl via industry-standard X.509 certificates issued by NetAuthority. ClearTrust SecureControl's security policy management infrastructure (PMI) streamlines authorization by enabling users to sign on once for access to any number of Web applications instead of having to rely on separate usernames and passwords for each, regardless of operating platform. In addition to bolstering security, the PMI, which can be configured to limit access to pre-determined applications, reduces the costs associated with replacing forgotten or otherwise obsolete usernames and passwords. NetAuthority provides the trusted environment for user authentication to PMI and a number of other Internet-based applications.

"The Cylink-Securant solution will combine two compelling sets of features to provide the security needed for highly trusted web-based communications," said William P. Crowell, President and CEO of Cylink. "The strong user authentication of Cylink's NetAuthority PKI and the central access control of Securant's security policy management infrastructure will provide an easy-to-use platform for tailoring access to Internet applications."

"As enterprises move high-value transactions and business-critical applications onto the Internet, PKI provides the level of trust and security required to protect these sensitive resources from misuse and fraud," said Eric Olden, Securant's Chief Technology Officer. "The integration of Cylink's NetAuthority solution with our ClearTrust SecureControl access management system will maximize the authentication capabilities of PKI and give enterprises the confidence to provide single sign-on Web access to precious applications and resources."

NetAuthority is a highly scalable, standards-based infrastructure incorporating public-key cryptography, certificates, digital signatures and encryption to enable a wide variety of applications including secure email and web browsing and virtual private networking. Designed to support intranet, extranet and Internet applications, NetAuthority consists of a certificate authority, registration server, registration authority client and a toolkit that can make any device and application PKI-compatible.

ClearTrust SecureControl enables enterprises to centrally manage PKI-based authentication to protect both Web-based and Web-presented applications. In addition, ClearTrust SecureControl can manage and deliver multiple security services that integrate with PKI. To provide real-time security enforcement and prevent unauthorized access, the PMI solution supports Certificate Revocation List (CRL) checks to deny access to users with revoked or suspended certificates.

About Securant

Securant Technologies, the access management company that secures e-business, is a leading provider of Internet security software for managing user access to Web-based resources including applications, content and transactions. Securant customers include Merrill Lynch, Baker Street, Chase Hambrecht & Quist, Lehman Brothers, Experian, MarketFusion,

Scientific Atlanta and Thomson Financial. To contact Securant, call 415/315-1500, visit www.securant.com, or write to info@securant.com.

About Cylink Corporation

Cylink Corporation develops, markets and supports a comprehensive family of e-business security solutions. Founded in 1983, the company was the first to market security solutions that protect communications with public key cryptography. Cylink and its wholly owned subsidiaries serve Fortune 500 companies, multinational financial institutions, and government agencies worldwide. To contact Cylink, call 408/855-6000 or visit www.cylink.com.

Some of the statements in this announcement involve risks and uncertainties, and actual results could be materially different. The statements concerning the parties' future product offerings and their capabilities are forward looking statements. Among the factors that could cause actual results or developments to differ are unexpected delays in product developments, failure of the market to accept new products or technologies, difficulty in hiring and retaining qualified personnel, and other risk factors listed from time to time in the company's SEC reports, including but not limited to the report on Form 10-K, Forms 10-Q, and the Annual Report to shareholders.

Note to Editors: Cylink is a registered trademark of Cylink Corp.

CONTACT: Cylink Corp. Mike Hall, 408/855-6390 mhall@cylink.com or S&S Public Relations Steve Simon, 800/287-2279 steve@sspr.com or Marc Gendron PR (For Securant) Marc Gendron, 781/237-0341 marc@mgpr.net

08:04 EST MARCH 12, 2001

COUNTRY NAMES/CODES: United States of America (US)
REGIONS: Americas; North America; Pacific Rim
PROVINCE/STATE: California
SIC CODES/DESCRIPTIONS: 7372 (Prepackaged Software)
NAICS CODES/DESCRIPTIONS: 51121 (Software Publishers)

1/9/6 (Item 3 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

08129562 (THIS IS THE FULLTEXT)
Reasons for Federal List Losses Analyzed
Article Anna Kozyreva: "Someone Has a Horse With Just Three Legs. And the Horse Is Missing..."
WORLD NEWS CONNECTION
November 04, 1999
JOURNAL CODE: WWNC LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 720

As has already been reported, not all the electoral associations and blocs made it to the home stretch. But whereas the NUR association was simply denied registration, the decision was made to turn over the National Salvation Front's signature lists to the prosecutor's office, as the members of the Central Electoral Commission (CEC) felt that "some fraud had occurred." More than 21.07% of the signatures were declared unsubstantiated, and under the law having 15% of signatures in that category is grounds for denial of registration. In addition it was discovered that the passports, the numbers of which were indicated in the signature lists, simply do not exist in Russia.

Virtually all the associations' federal slates suffered major losses. Many party comrades did not make the cut because in their income and

property statements those comrades submitted information "the unreliability of which is substantial." You can debate over whether or not a 1968-vintage automobile is property and how much it is worth, but the law is the law. Candidates for deputy are even required to list that heap of scrap metal. Yet during CEC sessions everyone was forced to listen to endless lists of undeclared automobiles of every make and model on earth, with the members of the associations all attempting to prove that "I'm not me and that horse is not mine." "Oh, that Zhiguli is really, really old, it's all rusted out, and it sits outside rotting away, and my Audi was stolen a long time ago, and they still haven't found it." This was the endless lament heard day after day at the CEC sessions.

For instance, Vladivostok's Mayor Cherepkov, who did not list his two Nissans, was dropped from the slate of the Bloc of General Andrey Nikolayev and Academician Svyatoslav Fedorov. General Ochalov from the DPA met the same fate and had his registration revoked for not indicating that he owned a Volvo and a Mercedes-Benz. Leader Viktor Ilyukhin found all this very upsetting.

One citizen named Vyguzov almost had his registration revoked because he did not list his dacha. But his colleagues managed to prove that the tiny house was only worth... 59 rubles. Vyguzov's documents were sent back for reexamination. Another loser was television host Arina Sharapova. She was also dropped from the slate. She had not listed her supplementary income of R14,000. But the Medved bloc did not come to her defense. As Aleksandr Gurov (number three on the Medved slate) summed it up: "they were idiots, such idiots!" Vladimir Zhirinovskiy did manage to register his bloc, which is in fact the same old LDPR, on his second attempt. The Liberal Democrats did not lose a single one of their members in the process. Furthermore, the "Zhirinovskiy Bloc" is the only bloc whose candidates for deputy actually listed property that is not registered anywhere else and cars that the State Motor Vehicle Inspection does not have in its records. Vladimir Volfovich explained his colleagues' odd behavior by quoting an old Russian saying: "Once you've been burned by milk, you even blow on water." The sensation of the week was registration of a candidate slate from the Spas association. As you may recall, the number one spot on the slate belongs to Aleksandr Barkashov, leader of the RNE. But since the Ministry of Justice has not yet managed to "repeal" the RNE, there were no grounds to deny CEC registration, although, as CEC Chairman Aleksandr Veshnyakov commented, "his hand shook" as he signed the Spas lists. But Spas' political views are not grounds for denial; after all, not everyone cares for the views of the CPRF or Fatherland-All Russia...

In recent days the CEC's work has turned up another curious item.

Simultaneously two associations - the Bloc of General Andrey Nikolayev and Academician Svyatoslav Fedorov and Spas - paid campaign deposits, the money for which was drawn from the personal funds of members of those associations. Here is the curious part: they each deposited R25,000 apiece from 100 individuals. Aleksandr Veshnyakov proposed that an auditing service look into this situation. There are concerns that the money had simply been handed out to party members, and that we are seeing "an attempt to launder money in this fashion."

DESCRIPTORS: Law & Legal Issues; General News; Elections; Government News
COUNTRY NAMES/CODES: Russia (RU)
REGIONS: Commonwealth of Independent States; Former USSR

SIC CODES/DESCRIPTIONS: 9222 (Legal Counsel & Prosecution)
NAICS CODES/DESCRIPTIONS: 92213 (Legal Counsel & Prosecution)

1/9/9 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

13355316 SUPPLIER NUMBER: 73376164 (THIS IS THE FULL TEXT)
E-Signed, Sealed, and Delivered.
Piazza, Peter
Security Management, 45, 4, 72
April, 2001
ISSN: 0145-9406 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 3637 LINE COUNT: 00285

TEXT:

Two very different institutions roll out public key infrastructures to authenticate users and protect confidential information.

PUBLIC KEY INFRASTRUCTURE (PKI). The mere name of this authentication and encryption system can make the average business person's eyes glaze over. Even among the techno-literate, PKI has an enduring reputation as hard to understand and even harder to implement. But Chrisan Herrod of Fannie Mae is a PKI fan. "It's something that can help you if you let it help you, and you can change your business processes using it," says Herrod, director of information security at Fannie Mae. She should know. She oversaw the rollout of a PKI system at her company, the largest provider of home mortgages funds in the United States. The Massachusetts Institute of Technology (MIT) went through a similar rollout of its own PKI system. The two experiences offer valuable lessons to businesses looking for ways to secure online transactions.

MIT's School Project

TO REGISTER FOR CLASSES, STUDENTS AT MIT, LIKE students everywhere, have in the past had to fill out forms on paper, then stand in long lines in the gym to submit their forms to the registrar. When a class they wanted was fully subscribed, they had to go back to the end of the line, frantically thumbing through paper catalogs to find replacement courses as they made their way again to the front of the line. Meanwhile, the registrar's staff working the lines had to manually enter the information for 10,000 students into the university's computer database. It was tedious and exasperating for everyone involved.

Assessing needs. Administrators knew that there must be a more efficient way to get students registered. They decided to set up a Web-based system to allow students to preregister for classes by computer. The question was how to make it secure. The answer was PKI, because it offered two critical capabilities: privacy and authentication.

Blessed with state-of-the-art technology and no shortage of scientific minds, the university created a system from scratch, rather than outsourcing the project, as most businesses would. However, MIT's experience in assessing how PKI could benefit them and rolling out the system to thousands of users can be a lesson for any business.

The school's needs were fairly simple, according to Jeffrey Schiller, network manager and security architect for MIT. Students needed a way to prove their identity to register for classes and access the university Web sites, and the university needed a way to ensure that private data on the site, such as financial aid or grades, would be secure.

PKI startup. It took Schiller about a week to write code for the PKI system, which is based on the idea of digital certificates, issued as a form of electronic ID, and public/private key pairs, issued for encryption and decryption. In a PKI System, there must be a trusted relationship with

a third party, so that individuals or systems have a basis for trusting each other's messages over a network. Thus, there are three pieces to the PKI puzzle when it comes to the issuance of certificates: the root certificate authority (RCA), the certificate authority (CA), and the end user, which gets issued the certificate and public/private digital key pair. In MIT's case, the university is the CA.

While MIT issues certificates to students, the university itself has been issued a certificate by an RCA, which also happens to have its server on MIT's property. That RCA is called CREN (the Corporation for Research and Educational Networking, a consortium of universities that provides institutional certificate services). CREN certificates are issued when a school registers to be a CA.

The authority to be a CA and issue digital certificates must be carefully controlled if digital certificates are to be trusted forms of identification in the electronic universe. Thus, the server that issues the CREN root certificates is secured inside a hardware box in a locked, alarmed room on MIT's campus. Schiller explains that the CREN server requires an extremely high level of security because if an unauthorized person obtained access, that person could become a CA with the ability to issue digital certificates to anyone--essentially manufacturing fake electronic IDs.

To ensure against the possibility of an unauthorized CA root certificate being issued, the CREN server cannot sign a certificate unless two people insert plastic "crypto-ignition" keys (similar to those used for firing missiles from submarines) at the same time. Schiller has one, kept under two levels of lock and key; the other is similarly secured by the director of academic computing at MIT.

Another part of the picture is an institutional digital key, used by MIT to issue certificates to students. "The tricky part," Schiller says, "is that the server that issues certificates to people is an online service." This unavoidably creates a level of insecurity. This key is encrypted, and though Schiller has made it difficult to steal, he acknowledges that "somebody sufficiently skilled in the arts" could do it. He adds that MIT runs its own network-level intrusion detection system so that the university would be immediately aware of and able to respond to any unauthorized access to the server.

Pilot program. The university tested its electronic ID system in 1996 with a short pilot program involving about 100 students. The pilot went smoothly, and MIT rolled out the system to another 8,000 students that summer.

All of the participating students received a paper coupon when they arrived on campus, with their name, identification number, and a unique six-word passcode. They used this passcode to access a special MIT Web site residing on the server that was the nerve system of the CA function; once they entered the passcode, which proved their identity, they chose a new user name and password. An automated program (called a wizard) then led the students through a simple process to receive two packets of data that would be used by computers on either side of future transactions to verify the student and the site.

These packets are called digital certificates. Both reside in the browser of the student's computer. The first is an MIT site certificate, which certifies the identities of MIT sites on the Internet. The second packet is a personal certificate, which contains the student's name, the student's user name, the beginning and expiration dates of the certificate, and a certificate serial number. The certificate-holder also gets a public/private key pair. A digital signature, encrypted with the private key, becomes an electronic ID because it can only be decrypted by the corresponding public key.

The student's private key resides on his or her computer, and the student has a password to retrieve it. If anyone obtains the password and

gains access to the private key, he or she can impersonate the student.

"That's the weakest link," Schiller says. "However, the tradeoff is that it only affects one person." MIT tells students not to share that information with anybody and that violators of the policy will be held responsible for any negative results.

How it works, If student John Smith wants to check his grades, he'll point his browser to the designated MIT Web site. When he reaches the page, the Web site will challenge his browser to provide John's certificate. If he hasn't used the certificate before in this session, he'll be prompted to enter the password that protects the certificate. This extra safeguard helps to ensure that someone else could not sit at John's computer and impersonate him electronically.

Meanwhile, John's browser will check the MIT site certificate to verify the identity of the site. Through this digital "handshake," both John and the Web site provide authentication of their identities.

Next, the Web server takes John's user name from the certificate and matches it (through an internal database) to his student identification number. Based on that identification, the computer presents him with his records. During this process, John never sees the certificates being used; the process is automatic.

The certificates enable students to use their computers to enter class and housing lotteries, gain access to online libraries and journals, and purchase items at a discount from certain online vendors. The certificates are accepted by third-party vendors, so employees can also use them to purchase office supplies and computer products.

Rollout problems. Unlike many other enterprise PKI projects, MIT moved from pilot to full implementation quickly--in the course of one semester--and with great success. "We've had maybe 100 problems, but we've issued 200,000 certificates," Schiller says, "and that's not a bad ratio." Most of the problems were not serious and involved error messages or crashes caused by improperly configured browsers. A help desk Web site allows users to solve those problems easily.

Key compromise. So far, Schiller says, no student has ever reported the compromise of a private key, but he suspects that may be because students do not understand the need to have the certificate revoked if, for example, a laptop is stolen.

He suspects some laptops have been stolen, "so some have had their keys compromised," he says. "End users don't understand that they have to take an action" by immediately reporting it to the systems administrator so the certificate can be revoked and reissued. The university is trying to address the issue through education.

Key management. Key management is a major issue in the administration of a PKI program. Making students aware of the need to report stolen or compromised keys is only one part of the key management challenge. If a student quits the university, MIT will revoke the corresponding certificate. However, that student still has the certificate on his or her computer. It could not be used to log into the registrar's office or access any sensitive sites within MIT. But an outside vendor that had been approached online would have to check a certificate revocation list to know that it should deny the transaction. This is more of a problem with employees whose certificates have been revoked. "If a staff member leaves, we want to make sure they can't go and buy a computer" using their MIT certificate, Schiller says.

Schiller anticipates that some difficulties might also arise when certificates are used among institutions. He explains how different authentication policies can lead to mistrust. "For example, we give (students) a coupon when they arrive that allows them to get a certificate. Another university might decide that a student has to appear before a university official with two forms of picture ID and a notarized statement. The problem is, would that university accept a credential issued by MIT?"

Schiller is not sure how such conflicts will be resolved, He notes that for now the university simply indicates on the certificate how the student's identity was authenticated so that others can make an informed decision about its validity.

Results. Mary Callahan, the registrar of MIT, says that the university has found the effort worthwhile. "Students get a lot more good information online, right in front of them. We can update (the site) if a subject changed its time or got cancelled, so a student gets the most current information, rather than a time-dated paper bulletin."

The new system has also saved her staff from hours of tedious data entry. "Now we do a lot more problem solving," she says. "I feel that we offer a lot better level of service, but it takes a different skill set now to be working in the registrar's office."

Targeted PKI

THE FIRST QUESTION THAT FACED FANNIE Mae when it began to consider the use of an electronic ID system was how extensively to implement PKI. "You don't have to PKI your whole company," Director of Information Security Herrod says. "A lot of people go overboard."

To handle the project, the company assembled a team that included members of the operations, legal, human resources, network engineering, and ebusiness departments. The group examined the company's needs and requirements, present and future, to determine exactly what should be protected by the authentication and encryption capabilities that PKI would provide.

The project team came to several conclusions. First, the company wanted secure e-mail and intranet applications for internal use. Second, it needed to protect sensitive employee data and confidential information about customers. General e-mails about policies or nonsensitive data would not need to be encrypted or digitally signed.

The team also decided to use PKI to streamline transactions. "PKI not only provides encryption but (also) provides the ability to 'sign on the digital line,' so we can sign timecards online," Herrod says. "In the future we can sign purchase orders online, too. We can reduce the workflow tremendously and hence reduce costs and increase efficiencies as well."

The next step was to select a PKI partner. The team created a list of essentials. First, the secure e-mail and any Web-based applications would have to work with Netscape and Microsoft Outlook, which was already standardized in the company. Looking into the future, they wanted to be able to implement a secure remote access method called virtual private network, or VPN, using smart cards or tokens, as well as desktop encryption. They needed a simple rollout that was easy for users and administrators. Finally, they wanted their PKI system to be up and running quickly. The team sent its needs to several PM vendors. These suppliers then gave presentations. Eventually, the company chose to outsource the project to Entrust.

Starting small. Fannie Mae decided that the best course of action would be to set up an internal PKI system first, and once the infrastructure was working smoothly, to push that out to private lenders, real estate agents, and others who work with the company. By focusing on an internal PKI system first, Herrod and her team could be sure that they completely understood the technology and that they could work through any glitches before getting into client considerations.

Even within the company, Herrod found, the process should he gradual. "Experiment with your rollout procedures before you actually give it to important users in your company," she says. "I would never start with the CEO; always start out with your own team first."

Because it needed an easy-to-use system that was up and running quickly, Fannie Mae decided that Entrust would take care of all the backend infrastructure; it hosted the certificates and set up the policy configuration according to Fannie Mae's needs. Fannie Mae's users and

administrators would securely access the certificates through the Web.

Certificate policy. The Fannie Mae team established a certificate policy (CP) and a set of rules addressing concerns such as the CA's key length and how long the certificates would be valid. This CP, says Leah MacMillan, director of product management and marketing for Entrust, made the implementation much easier. "We could look at the CP and make sure that we conformed to everything that they needed to do. Then we could explain how we were going to set up their PKI according to their security policies and desired configuration settings."

Entrust brought a small group of Fannie Mae users to its lab, where a sample system based on the CP was set up. The users checked out all the settings to make sure they were in accordance with what was expected, learned the administrative functions, and saw what kinds of problems arose before the system went live.

The PKI system is integrated with the Netscape browser and Microsoft Outlook e-mail application on each desktop. At first, there were some computer crashes, but these were not completely unexpected, Herrod says. "If you don't have the browser properly configured, you'll have a problem, and it happens quite a bit, no matter what vendor you're using," she says.

Herrod's team realized they needed to change certain Netscape browser security configurations on every desktop to prevent the crashes. They developed an automated script and distributed it via e-mail to users, who only had to double-click on the message to launch a silent install, which would change the browser settings.

Entrust support staff spent about a week in the company, training the system administrators on how to use the system. Two Fannie Mae staff members were given additional duties as registration authorities (RAs), administrators who add and delete users from the system. The RAs completed a short training course in how to load and delete information. Once the RAs received their digital IDs, they could begin to add new users; they could also assign and create additional local RAs to distribute the administrative work as the system expanded.

Two other staff members were designated as revocation authorities. If someone loses a laptop or leaves the company, they revoke the certificate instantly.

Testing. Fannie Mae's RAs selected 500 users to register for digital certificates as a part of a test. Users were selected from departments, such as HR and legal, whose staff handled the type of transactions that would merit PM security. The RAs sent an e-mail to these users welcoming them and informing them that they would be prompted for a password to get the certificate. (The e-mail explained that the password would be a piece of identifying information that the employee and the registrar would both know but that would not be common knowledge. For example, they might he asked for their mother's maiden name.)

The e-mail then directed each user to click on the Web site address in the message. This launched the browser, and the Web page that opened asked the pilot users to enter their password to begin the creation of their digital ID. The site securely accesses Entrust, which issues and stores their certificates, and the Entrust software in the browser generates public and private keys, which give users the ability to encrypt and sign online. The private key is password protected in the user's browser.

Training. Next, Fannie Mae instituted a training class for its pilot group of 500 users. Trainers explained to the employees who would be issued the certificates exactly why the PKI system was implemented and how it would work. For example, they were told that once they received their certificates, they would simply click on an icon to activate the encryption routine or to digitally sign a document. If an encrypted e-mail arrived, users would simply double-click on it, and the process would occur.

In addition to the training class instituted, Fannie Mae has put

information on its Web site that walks users through its policy on when to use-- and when not to use--encryption. For example, human resources personnel are told to encrypt messages containing salary data, legal information, and medical data. Users are taught to apply PKI based on commonsense rules and practices, Herrod explains. They are told: "If you think this is too sensitive to send via e-mail, then encrypt it," she says.

Rollout. One of Fannie Mae's long-term goals is to encrypt sensitive records and restrict user access to that data, using the same PKI system. "Privacy is a huge issue, and we want to make sure that we're protecting private information," says Herrod. "We have tremendous databases where we store information about homebuyers, and that's something we're obligated under the law to protect."

To give staff a chance to try out their certificates, Fannie Mae posted its code of conduct on a Web site, and each user digitally signed it. As the company rolls out the program to the rest of the staff, it has set up lunchtime learning sessions by department to walk users through the encryption feature. The training and the rollout are continuing incrementally, and by the end of 2002, every full-time Fannie Mae employee--about 4,000 people--will have a certificate. In the future, the company intends to use smart cards or tokens rather than passwords to enhance the security of the user's private key.

Future impact. Fannie Mae is working with the Mortgage Bankers Association of America and the American Bankers Association to create the Real Estate Finance (REF) Trust Network, a community-of-interest certificate authority on behalf of the real estate finance industry. Through the REF Trust Network, certificates can be issued to accredited institutions that can then do e-business together.

PKI makes business more efficient, Herrod says. That, she notes, will eventually benefit homebuyers as well by creating a paperless mortgage application process.

As these case studies illustrate, setting up electronic ID and encryption systems can be a challenge. But the rewards of automating such routine tasks as student registration and loan applications can pay great dividends down the digital road.

Peter Piazza is assistant editor of Security Management.

COMPANY NAMES: Federal National Mortgage Association--Safety and security measures
INDUSTRY CODES/NAMES: BUSN Any type of business; ENG Engineering and Manufacturing; LAW Law
DESCRIPTORS: Massachusetts Institute of Technology--Safety and security measures; Mortgage banks--Safety and security measures; Universities and colleges--Safety and security measures; Security systems--Management
GEOGRAPHIC CODES/NAMES: 1USA United States
PRODUCT/INDUSTRY NAMES: 6160000 (Mortgage Bankers & Brokers); 8220000 (Colleges & Universities)
SIC CODES: 6160 Mortgage Bankers and Brokers; 8221 Colleges and universities
NAICS CODES: 52231 Mortgage and Nonmortgage Loan Brokers; 61131 Colleges, Universities, and Professional Schools
TICKER SYMBOLS: FNM
FILE SEGMENT: TI File 148

1/9/10 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

13191111 SUPPLIER NUMBER: 71554994 (THIS IS THE FULL TEXT)
Cylink, Securant to Offer Integrated PKI-based Solution To Bolster Web

Security.
Business Wire, 2132
March 12, 2001
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 795 LINE COUNT: 00076

TEXT:

Business Editors/High-Tech Writers

SANTA CLARA, Calif.--(BUSINESS WIRE)--March 12, 2001

Cylink's NetAuthority PKI and Securant's ClearTrust SecureControl to Provide Central, Tailored Access of Web-based Applications

Cylink Corporation (Nasdaq:CYLK), a leading provider of e-business security solutions, has partnered with Securant Technologies to offer an integrated public key infrastructure-based solution that allows enterprises, government agencies and application service providers to centrally control and tailor access to Internet-based applications, content and transactions.

Under the agreement, Cylink will ensure that its NetAuthority public key infrastructure (PKI) solution is compatible with Securant's ClearTrust SecureControl access management system. The integrated solution will provide enterprises with a single auditable point of control for managing access to PKI-secured Internet and extranet applications for employees, customers and partners.

Using easy-to-follow on-screen instructions, users of the integrated solution will authenticate to ClearTrust SecureControl via industry-standard X.509 certificates issued by NetAuthority. ClearTrust SecureControl's security policy management infrastructure (PMI) streamlines authorization by enabling users to sign on once for access to any number of Web applications instead of having to rely on separate usernames and passwords for each, regardless of operating platform. In addition to bolstering security, the PMI, which can be configured to limit access to pre-determined applications, reduces the costs associated with replacing forgotten or otherwise obsolete usernames and passwords. NetAuthority provides the trusted environment for user authentication to PMI and a number of other Internet-based applications.

"The Cylink-Securant solution will combine two compelling sets of features to provide the security needed for highly trusted web-based communications," said William P. Crowell, President and CEO of Cylink. "The strong user authentication of Cylink's NetAuthority PKI and the central access control of Securant's security policy management infrastructure will provide an easy-to-use platform for tailoring access to Internet applications."

"As enterprises move high-value transactions and business-critical applications onto the Internet, PKI provides the level of trust and security required to protect these sensitive resources from misuse and fraud," said Eric Olden, Securant's Chief Technology Officer. "The integration of Cylink's NetAuthority solution with our ClearTrust SecureControl access management system will maximize the authentication capabilities of PKI and give enterprises the confidence to provide single sign-on Web access to precious applications and resources."

NetAuthority is a highly scalable, standards-based infrastructure incorporating public-key cryptography, certificates, digital signatures and encryption to enable a wide variety of applications including secure email and web browsing and virtual private networking. Designed to support intranet, extranet and Internet applications, NetAuthority consists of a certificate authority, registration server, registration authority client and a toolkit that can make any device and application PKI-compatible.

ClearTrust SecureControl enables enterprises to centrally manage PKI-based authentication to protect both Web-based and Web-presented applications. In addition, ClearTrust SecureControl can manage and deliver

multiple security services that integrate with PKI. To provide real-time security enforcement and prevent unauthorized access, the PMI solution supports Certificate Revocation List (CRL) checks to deny access to users with revoked or suspended certificates.

About Securant

Securant Technologies, the access management company that secures e-business, is a leading provider of Internet security software for managing user access to Web-based resources including applications, content and transactions. Securant customers include Merrill Lynch, Baker Street, Chase Hambrecht & Quist, Lehman Brothers, Experian, MarketFusion, Scientific Atlanta and Thomson Financial. To contact Securant, call 415/315-1500, visit www.securant.com, or write to info@securant.com.

About Cylink Corporation

Cylink Corporation develops, markets and supports a comprehensive family of e-business security solutions. Founded in 1983, the company was the first to market security solutions that protect communications with public key cryptography. Cylink and its wholly owned subsidiaries serve Fortune 500 companies, multinational financial institutions, and government agencies worldwide. To contact Cylink, call 408/855-6000 or visit www.cylink.com.

Some of the statements in this announcement involve risks and uncertainties, and actual results could be materially different. The statements concerning the parties' future product offerings and their capabilities are forward looking statements. Among the factors that could cause actual results or developments to differ are unexpected delays in product developments, failure of the market to accept new products or technologies, difficulty in hiring and retaining qualified personnel, and other risk factors listed from time to time in the company's SEC reports, including but not limited to the report on Form 10-K, Forms 10-Q, and the Annual Report to shareholders.

Note to Editors: Cylink is a registered trademark of Cylink Corp.

COMPANY NAMES: Cylink Corp.
INDUSTRY CODES/NAMES: BUS Business, General; BUSN Any type of business
DESCRIPTORS: Telecommunications equipment industry
GEOGRAPHIC CODES/NAMES: 1USA United States
PRODUCT/INDUSTRY NAMES: 3662000 (Communications Equipment ex Telephone)
SIC CODES: 3660 Communications Equipment
NAICS CODES: 3342 Communications Equipment Manufacturing
TICKER SYMBOLS: CYLK
FILE SEGMENT: NW File 649

1/9/12 (Item 1 from file: 621)

02829948 Supplier Number: 71554994 (THIS IS THE FULLTEXT)

Cylink, Securant to Offer Integrated PKI-based Solution To Bolster Web Security.

Business Wire, p2132
March 12, 2001
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 795

TEXT:

Business Editors/High-Tech Writers

SANTA CLARA, Calif.--(BUSINESS WIRE)--March 12, 2001

Cylink's NetAuthority PKI and Securant's ClearTrust SecureControl to Provide Central, Tailored Access of Web-based Applications

Cylink Corporation (Nasdaq:CYLK), a leading provider of e-business security solutions, has partnered with Securant Technologies to offer an integrated public key infrastructure-based solution that allows enterprises, government agencies and application service providers to centrally control and tailor access to Internet-based applications, content and transactions.

Under the agreement, Cylink will ensure that its NetAuthority public key infrastructure (PKI) solution is compatible with Securant's ClearTrust SecureControl access management system. The integrated solution will provide enterprises with a single auditable point of control for managing access to PKI-secured Internet and extranet applications for employees, customers and partners.

Using easy-to-follow on-screen instructions, users of the integrated solution will authenticate to ClearTrust SecureControl via industry-standard X.509 certificates issued by NetAuthority. ClearTrust SecureControl's security policy management infrastructure (PMI) streamlines authorization by enabling users to sign on once for access to any number of Web applications instead of having to rely on separate usernames and passwords for each, regardless of operating platform. In addition to bolstering security, the PMI, which can be configured to limit access to pre-determined applications, reduces the costs associated with replacing forgotten or otherwise obsolete usernames and passwords. NetAuthority provides the trusted environment for user authentication to PMI and a number of other Internet-based applications.

"The Cylink-Securant solution will combine two compelling sets of features to provide the security needed for highly trusted web-based communications," said William P. Crowell, President and CEO of Cylink. "The strong user authentication of Cylink's NetAuthority PKI and the central access control of Securant's security policy management infrastructure will provide an easy-to-use platform for tailoring access to Internet applications."

"As enterprises move high-value transactions and business-critical applications onto the Internet, PKI provides the level of trust and security required to protect these sensitive resources from misuse and fraud," said Eric Olden, Securant's Chief Technology Officer. "The integration of Cylink's NetAuthority solution with our ClearTrust SecureControl access management system will maximize the authentication capabilities of PKI and give enterprises the confidence to provide single sign-on Web access to precious applications and resources."

NetAuthority is a highly scalable, standards-based infrastructure incorporating public-key cryptography, certificates, digital signatures and encryption to enable a wide variety of applications including secure email and web browsing and virtual private networking. Designed to support intranet, extranet and Internet applications, NetAuthority consists of a certificate authority, registration server, registration authority client and a toolkit that can make any device and application PKI-compatible.

ClearTrust SecureControl enables enterprises to centrally manage PKI-based authentication to protect both Web-based and Web-presented applications. In addition, ClearTrust SecureControl can manage and deliver multiple security services that integrate with PKI. To provide real-time security enforcement and prevent unauthorized access, the PMI solution supports Certificate Revocation List (CRL) checks to deny access to users with revoked or suspended certificates.

About Securant

Securant Technologies, the access management company that secures e-business, is a leading provider of Internet security software for managing user access to Web-based resources including applications, content and transactions. Securant customers include Merrill Lynch, Baker Street,

Chase Hambrecht & Quist, Lehman Brothers, Experian, MarketFusion, Scientific Atlanta and Thomson Financial. To contact Securant, call 415/315-1500, visit www.securant.com, or write to info@securant.com.

About Cylink Corporation

Cylink Corporation develops, markets and supports a comprehensive family of e-business security solutions. Founded in 1983, the company was the first to market security solutions that protect communications with public key cryptography. Cylink and its wholly owned subsidiaries serve Fortune 500 companies, multinational financial institutions, and government agencies worldwide. To contact Cylink, call 408/855-6000 or visit www.cylink.com.

Some of the statements in this announcement involve risks and uncertainties, and actual results could be materially different. The statements concerning the parties' future product offerings and their capabilities are forward looking statements. Among the factors that could cause actual results or developments to differ are unexpected delays in product developments, failure of the market to accept new products or technologies, difficulty in hiring and retaining qualified personnel, and other risk factors listed from time to time in the company's SEC reports, including but not limited to the report on Form 10-K, Forms 10-Q, and the Annual Report to shareholders.

Note to Editors: Cylink is a registered trademark of Cylink Corp.

PUBLISHER NAME: Business Wire
COMPANY NAMES: *Cylink Corp.
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *3662000 (Communications Equipment ex Telephone)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
SIC CODES: 3660 (Communications Equipment)
NAICS CODES: 3342 (Communications Equipment Manufacturing)
TICKER SYMBOLS: CYLK
?